하드웨어 친화적인 암호 알고리즘을 사용한 RFID 프라이버시 보호 시스템

김진묵* · 유황빈*

*광운대학교 컴퓨터과학과

A RFID Privacy protection system using H/W friendly security algorithm Environment

Jin-mook Kim* · Hwang-bin Ryou*

*Department of Computer Science, Kwangwoon University

E-mail : jmkim@netlab.kw.ac.kr, ryou@kw.ac.kr

요 약

유비쿼터스 컴퓨팅 환경에서는 사물의 인식을 위해 바코드 시스템을 대체하여 RFID 시스템이 사용될 것으로 예상된다. 하지만 RFID 시스템은 태그와 리더 사이에서 프라이버시 침해 문제가 심각할 것으로 예상된다. 하지만 이를 해결하기 위해 기존의 연구방법을 그대로 적용하기에는 태그가 가지고 있는 하드웨어적인 제약사항으로 인해 어려움이 많다.

본 논문에서는 하드웨어 친화적인 암호 알고리즘을 사용한 RFID 프라이버시 보호 시스템을 제안하고자 한다. 제안한 RFID 프라이버시 보호 시스템은 CBC_MAC과 RC5를 이용하여 태그가 가진 제약사항을 극복할 수 있다. 제안한 시스템의 구현을 위해서 온 칩 마이크로프로세서 환경에서 시뮬레이션 하고 실험결과를 살펴본다. 실험결과, CBC_MAC과 RC5를 이용해 RFID 시스템에 대한 프라이버시 문제를 해결할 수 있음을 보인다.

ABSTRACT

In ubiquitous computing environment, An RFID system will be the important way that recognizing an object instead of Bar-code system. But a privacy infringement problem is predicted between a tag and leader to be serious. There is many difficulty that just uses an existing research method because it has an Hardware restriction.

Therefore we will suggest that A RFID Privacy Protect system using Hareware friendly security algorithm. we will use RC5 and CBC_MAC because the tag has hardware restriction .To implement, We will simulate and test on One chip microprcessor environment. In the result of the experiment, We will know that a suggested system solves privacy problem on RFID system that it was using CBC-MAC and RC5 security algorithm.

키워드

RFID, Privacy, Secure Tag, EPC

I. 서 론

IT 환경이 빠른 속도로 발전하면서 대두되고 있는 유비쿼터스 환경에서는 모든 사물이 통신의 주체이며 객체로서 동작할 수 있다. 이에 기존의 컴퓨팅 환경과 달리 유비쿼터스 환경에서는 장치들이 스스로 정보를 수집하고 분석하여 처리할 수 있는 환경으로 변화할 것이다. 이는 우리의 생활을 좀 더 편리하고 유용하게 할 것이다. 하지만 이는 보안적인 측면에서 바라볼 때 현존하는 컴퓨팅 환경과 비교하여 보다 심각한 문제들을 발생시킬 것으로 예상된다.[5-7]

특히 개인의 프라이버시 문제가 심각하게 발생할 것으로 예상된다. 유비쿼터스 환경에서는 많은 정보들이 사용자가 인식하지 못하는 사이에 수집되고 여러 가지 형태로 가공되어 질 것이다. 이러한 과정에서 사용자의 개인 프라이버시 정보가 외부로 드러나게 된다.[1-4]

이에 유비쿼터스 환경에 알맞은 암호 관련 기술과 개인의 프라이버시 보호 기술의 발전에 대해 파악하고 적용하는 방법에 대한 이해가 필요하다.[8]

본 논문에서는 유비쿼터스 환경에서 RFID 시스템에서 발생할 것으로 예상되는 개인의 프라이버시 문제를 해결하기 위해 하드웨어 친화적인 암호 알고리즘들을 채택하여 저 사양의 하드웨어 제약사항을 지닌 RFID 시스템에 적용 가능한 프라이버시 보호 대책을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 선행연구들에 대해 살펴보기로 한다. 3장에서는 제안하는 RFID 프라이버시 보호 시스템에 대해 기술한다. 4장에서는 제안한 시스템의 보안적인 측면과 성능 측면에서의 분석을 다루고 마지막으로 5장에서 결론을 기술한다.

II. 관련연구

RFID 시스템은 사물의 인식을 위해 기존의 바코드를 대체하여 가장 시급하게 연구가 진행되어 현실 생활에 적용되고 있다.

하지만 이에 따른 보안상의 위협요소들을 충족하지 못한 상태이다. 그러므로 이에 대한 대책 마련을 위해 선행 연구가 수행되었다. 아래의 표 1은 RFID 시스템에 대한 보안관련 연구들을 나타내고 있다.

표 1. RFID 보안 관련 연구

구분	연구명	연구내용
태그 무력화	● 패러데이케이지 ● Active Jamming ● Kill command ● Blocker Tag	태그가 부착된 사물을 일정시점에서 사용할 수 없도록 만들거나 허용된 사용자에게만 읽혀지도록 태그의 응답을 방해하거나 막는 방법
대응 정보 응답법	● Hash Lock ● Hash Lock 확장	태그와 리더 사이의 통신에 직접적인 태그정보가 아닌 대응 정보를 사용하고자 하는 방법
암호화	● One-time pad ● Re-encryption	도청을 통해 정보를 취득한다고 해도 원하는 정보를 얻을 수 없도록 하는 것

정리된 도표에서 나타내고 있는 내용은 RFID 시스템의 보안과 관련한 모든 분야의 내용을 나타내고 있다. 위의 표 1에서 다루고 있는 내용 중에서 프라이버시 문제와 밀접한 관련을 가지고 수행된 연구 분야는 2가지 분야로 나누어 볼 수 있다.

2.1 대응정보를 전달하는 방법

대응 정보 전달기법은 다른 말로 "Hash Lock 기법"이라고 불린다. 이는 태그와 리더 사이의 통신에서 사용되는 태그 식별정보인 EPC code를 대신하여 임시 식별정보를 전달하거나 이와 유사한 정보를 전달하는 것으로 대신하고자 하는 방법이다.

대응 정보 전달하는 방법은 기본적으로 해쉬함수를 태그에 탑재하여야 하는데 이는 저가의 태그가 가지고 있는 하드웨어적인 제약 조건으로 인해 실제 구현이 어렵다.

또한 이를 더욱 발전시키고자 하는 다른 방법들도 결국은 하드웨어적인 제약사항이나 프라이버시 문제를 부분적으로만 해결할 수밖에 없는 실정이다.

2.2 암호 알고리즘을 적용하고자 하는 방법

RFID 시스템에 대해 보안 서비스를 제공하고 프라이버시 문제를 해결하고자 하는 또 다른 노력으로는 RFID 시스템의 주체인 태그에게 적합한 새로운 암호 알고리즘을 개발하고자 하는 노력이다. 이는 현재 활발하게 진행중에 있으며 아직까지 구체적인 결과를 제시한 바는 없다.

III. RFID 프라이버시 보호 시스템

3.1 시스템 구성

RFID 시스템의 프라이버시를 보호하기 위해서는 기존의 연구방법들을 고려해 볼 때, 태그가 가지는 하드웨어적인 제약 사항을 극복하는 것이 가장 중요하다. 이에 본 논문에서는 암호 알고리즘 중에서 적은 하드웨어 자원을 가지고도 보안성이 높은 하드웨어 친화적인 암호 알고리즘을 사용하여 프라이버시를 보호하고자 한다.

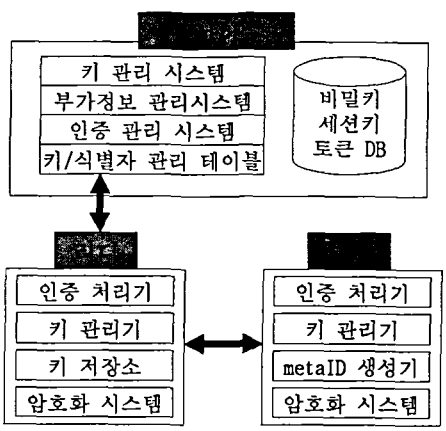

그림 1. 제안 시스템의 전체구조

제안하는 시스템은 EPC Global의 표준에 따라 Generation 1 Class 2 태그를 사용하는 시스템으로 구성한다. 이에 추가적으로 데이터를 암호화하기 위해 추가적인 저장 공간과 8 bit 프로세서를 탑재하고 있음을 가정한다.

시스템의 구성은 크게 서버와 리더, 그리고 태그 3개의 영역으로 구성된다. 이는 RFID 시스템의 기본 구성요소와 동일하다.

제안하는 시스템은 RFID 시스템에 대해 프라이버시 보호를 위해서 사전 키 분배를 위한 시스템[9-11], 태그와 리더 사이의 통신 과정에서 데이터를 암호화하기 위한 시스템, 태그와 리더가 다루는 정보를 암호화하기 위해 인증을 처리하는 시스템을 추가적으로 갖는다.

3.2 시스템 동작절차

제안하는 시스템은 3 단계를 동작절차를 갖는다. 먼저 리더와 태그 사이의 통신에서 사용되는 데이터에 대해 기본적인 보안 서비스를 제공하기 위해 암호화 처리를 할 때 필요한 비밀키를 생성하는 과정이 필요하다. 이를 위해 사전 키 분배 단계를 수행하게 된다.[] 이에 대한 과정을 아래의 그림 2 에 나타내고 있다.

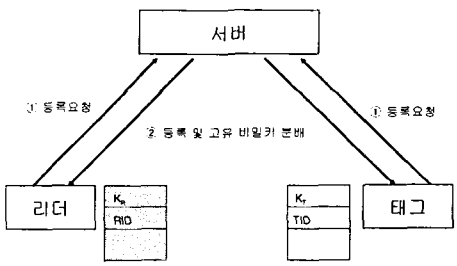

그림 2. 사전 키 분배 과정

두 번째로 태그와 리더 사이에 인증을 처리하는 과정을 수행하는 과정이 필요하다. 이에 대한 처리 과정을 아래의 그림 3 에 나타내고 있다.

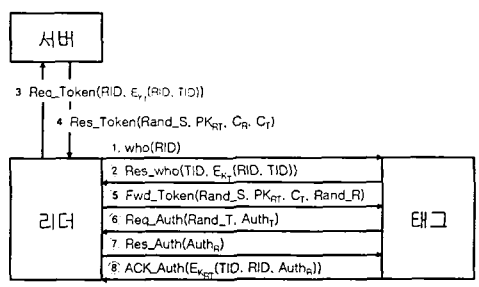

그림 3. 인증 처리 과정

마지막으로 실제로 태그와 리더 사이에서 데이터를 전송하고 태그에 대한 부가적인 정보를 요청하고 임시 식별자인 metaID를 생성 및 유지 관리하는 단계가 아래의 그림 4 에 나타낸다.

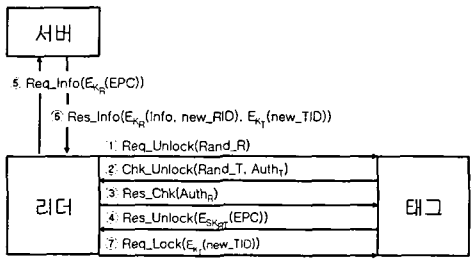

그림 4. 태그와 리더 사이의 통신 과정

위에서 살펴본 바와 같이 3 단계에 걸쳐 태그에 대한 임시 식별자를 태그가 생성하여 리더의 질문에 응답함으로써 태그에 대한 위치 추적 문제를 해결할 수 있다. 이때 CBC_MAC을 사용함으로써 기존의 해쉬 함수를 사용하는 방법이 태그의 처리 능력의 한계 조건으로 인한 문제를 해결 할 수 있다.

추가적으로 태그와 리더 사이의 통신 과정에서 기존에 제안된 공개키 기반의 암호 알고리즘을 사용할 수 없는 제약사항을 해결하고자 RC5 와 같은 하드웨어 제약 조건을 갖지 않는 하드웨어 친화적인 암호 알고리즘을 적용하고자 한다.

128bit 키 길이를 사용하고 16 라운드에 걸쳐 암호화를 수행한다고 하더라도 16 bit 단위의 워드를 처리하기 위해서 단순한 Shift rotate 연산과 XOR 연산만을 사용하는 RC5 암호 알고리즘은 매우 적은 하드웨어 자원을 요청한다. 그럼으로써 태그의 하드웨어적인 제약 사항으로 인해 동작할 수 없는 기존의 공개키 기반의 암호화 방식의 어려움을 해결할 수 있다.

IV. 성능 평가

4.1 실험환경

논문에서 제안한 시스템에 실험 평가를 위해 현재 생산되고 있는 RFID 시스템을 그대로 이용하기에는 아직은 무리가 따른다. 이에 RFID 시스템의 태그와 동작 환경이 유사한 원 칩 마이크로프로세서 시뮬레이터를 이용하여 처리 능력을 측정한다.

이를 위해 WinAVR 시뮬레이터를 이용하여 RFID 시스템의 패시브 태그가 갖는 환경과 유사한 환경으로 Atmel 사의 Atmega 128 칩 환경을 시뮬레이션 한다.

먼저 WinAVR을 이용해 암호 모듈과 대칭키 방식을 이용한 인증 모듈을 구현하고 이에 대한 처리 시간을 각각 측정하였다. 이를 살펴봄으로써 하드웨어적으로 제약사항을 갖는 태그 환경에서 암호화 처리 시간을 측정할 수 있고, 태그와 리더 사이에서의 처리 지연 시간을 측정할 수 있다.

4.2 실험 결과

4.2.1 안전성 평가

먼저 태그와 리더에서 암호화를 위해 사용하는 하드웨어 친화적인 암호 알고리즘인 RC5는 Rivest에 의해 제안된 알고리즘으로 현재 유선 네트워크 컴퓨팅 환경에서조차도 128 bit 키 길이와 시스템 단위의 word 길이, 16 라운드의 반복 처리 작업을 수행함으로써 안전성을 충분히 입증하고 있는 암호 체계이다. 더욱이 RFID 시스템과 같이 처리 대상이 작고 빠른 데이터 처리를 보장한다면 이에 대한 안전성은 충분히 보장 받을 수 있음을 예상할 수 있을 것이다.

두 번째로 태그와 리더 사이에서 암호화와 인증을 위해 Leighton에 의해 제안된 비밀키를 이용한 사전 키 분배와 인증 메커니즘을 적용함으로서 이에 대한 안전성을 충분히 증명이 가능하다.

세 번째로 프라이버시 문제에 대한 부분으로는 위치 추적 문제와 내용 프라이버시 문제에 대한 문제를 예로 들 수 있다. 위치 추적 문제에 대한 프라이버시 문제는 태그가 통신 세션마다 새로운 임시 식별자인 metaID를 사용해 리더와 통신함으로써 항상 리더들은 서로 다른 metaID를 할당 받기 때문에 태그에 대한 기존의 정보를 연속적으로 수집할 수 없음을 보일 수 있다. 또한 내용 프라이버시에 대한 문제는 태그가 평소에 잠금 상태로 metaID만을 응답하고, 잠금 상태 해제를 위해서는 인증과 별도의 처리 과정을 거쳐야만 가능함으로써 이를 증명할 수 있다.

지금까지 살펴본 바와 같이 제안한 시스템은 태그와 리더간의 통신에서 위치 추적 문제 및 내용 프라이버시 문제를 충분히 해결할 수 있고 추가적으로 기본적인 보안 서비스를 제공함으로써 비밀성 및 무결성을 보장할 수 있다.

4.2.2 성능 평가

제안한 시스템에 대한 성능 평가를 위해서 2가지 사항에 대한 처리 시간을 측정하였다.

WinAVR 시뮬레이터를 이용해 128bit EPC 코드를 갖는 패시브 태그를 시뮬레이션 하였다.

그리고 리더 부분을 위해서는 일반적인 PC 환경을 가정하기 위해 팬티엄 급 중앙 처리장치를 탑재한 환경에서 TinyOS를 설치하고 nesC를 이용해 에이전트를 구현하였다.

구분	암호화	복호화
RC5	482	490

표 2. 태그의 처리시간 측정결과(msec)

시뮬레이터를 이용해 구현한 태그에 대한 처리 능력을 측정하기 위해 96 bit EPC 코드체계에 padding을 하여 128 bit 단위의 데이터를 생성하고 이에 대한 암호화 및 복호화 처리 시간을 측정하였다. 이에 대한 처리 결과를 위의 표 2 에 나타낸다. 처리 단위는 mille second 이다.

다음으로 태그 시뮬레이터와 리더 환경간의 통신의 처리 지연시간을 측정하였다. 이에 대한 이해를 돕기 위해 일반적으로 동일한 키 길이와 라운드 수를 가지고 처리하는데 워드의 단위가 다른 PC 환경과 태그 시뮬레이터와 PC 환경의 처리 시간을 비교하여 표 3 으로 나타낸다.

구분	암호화	CBC_MAC
시뮬레이션	482	864
PC 환경	317	517

표 3. 태그와 리더 처리시간(msec)

위에 대한 실험 결과는 오차를 가질 수 있으나 동일한 실험 시나리오를 반복적으로 10 회 수행한 평균값을 나타낸 것이다.

실험 결과는 단일 태그와 리더 환경을 가정하여 처리 시간을 측정한 것으로 만약 리더와 태그의 개체수가 증가하게 된다면 이에 대한 처리 시간을 측정하기란 매우 어려울 것으로 예상된다.

하지만 위의 실험결과를 살펴봄으로써 기존의 PC 환경에 대비하여 그 처리시간이 느리기는 하지만 하드웨어 친화적인 암호 알고리즘과 MAC 생성 메커니즘을 적용함으로써 하드웨어 제약사항이 많은 RFID 시스템에서 안전한 데이터 처리를 통해 프라이버시 문제를 해결할 수 있음을 보인다.

V. 결론

유비쿼터스 환경이 도래함에 따라 RFID 시스템은 사물의 인식을 위해 기존의 바코드 시스템을 대체하는 가장 현실적인 대안으로 떠오르고 있다. 하지만 이에 대한 보안 문제가 기존의 유선 컴퓨팅 환경과 비교할 때 그 위험성이 매우 크다.

이에 본 논문에서는 RFID 시스템에서 발생할 것으로 예상되는 보안 문제 중에서 대표적인 프라이버시 문제를 해결하고자 RFID 시스템에 가지고 있는 하드웨어적인 제약사항을 극복할 수 있는 암호 알고리즘과 인증 메커니즘을 이용하여 위의 문제를 해결하고자 시도했다.

이에 대한 처리 결과를 시뮬레이션 결과를 얻음으로써 제안한 시스템에 대한 타당성과 현실적용 가능성을 가늠해 보았다. 하지만 제안한 시스템에 대한 성능 평가를 위해 실질적으로 RFID 시스템을 사용하는데는 어려움이 있어 원 칩 마이크로 프로세서 환경을 시뮬레이션 하여 얻을 결과로서 만족도가 적을 수 밖에 없다. 이는 향후 RFID 시스템의 태그의 성능에 대한 향상과 환경의 질적 향상을 이룬 후를 예상하면 충분히 묵과할 수 있을 것으로 예상된다.

또한 실험의 결과가 단일 태그와 리더 시스템을 가정하여 측정한 것으로 실질적인 환경에서는 이에 대한 처리결과가 매우 큰 값을 가질 것으로

예상된다. 이에 대한 부분은 향후 계속적인 연구를 통해 보완이 필요할 것이다.

참고문헌

[1] 강전일, 박주성, 양대헌, "RFID 시스템에서의 프라이버시 보호 기술", 한국정보보학회지, 제14권 6호, pp.28-36, 2004. 12.

[2] 곽진, 오수현, 이근우, 김승주, 원동호, "사용자 프라이버시 보호 및 추적이 가능한 EPC 시스템", 한국통신학회논문지, 제30권 1C, pp116-128, 2005. 01.

[3] 조정환, 여상수, 김성권, "AES를 기반으로 하는 개선된 RFID 프라이버시 보호 프로토콜", 한국컴퓨터종합학술대회 논문집, 제 32권 1A, pp.100-102, 2005.

[4] 유성호, 김기현, 황용호, 이필중, "상태기반 RFID 인증 프로토콜", 한국정보보호학회 논문지, 제 14권 6호, pp.57-67, 2004. 12.

[5] S. Sarma, S. Weis, and D. Engls, "RFID Systems, Security & Privacy Implications", AutoID Center. white Paper, 2002.

[6] S. Weis, "Security and Privacy in Radio-Frequency Identification Devices", MIT, May 2003

[7] S. Weis, S Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems", Security and Pervasive Computing 2003, LNCS 2802, pp.201-212.

[8] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to privacy-Friendly tags", in RFID Privacy Workshop, MIT, November 2003.

[9] T. Leighton and S. Micali, "Secret-Key Agreement without Public-Key Cryptography", Advances in Cryptology CRYPTO1993, pp.456-479, 1994.

[10] C. H. Lim, "Authenticated Key Distribution for Security Services in Open Networks", Technical Report, May 1997.

[11] M. Ramkumar, N. Memon, "security of random key pre-distribution schemes with limited tamper resistance", Mississippi Univ. 2004.